IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	
v.	**:**	**CRIMINAL NO. 09-424**
JING HE	**:**	

GOVERNMENT'S SENTENCING MEMORANDUM

The United States of America, by and through its attorneys, Michael L. Levy, United States Attorney for the Eastern District of Pennsylvania, and Leo R. Tsao, Assistant United States Attorney, hereby files, its sentencing memorandum.

Preliminary Statement

There can be little question that the defendant's crimes are very serious. During his one-year employment with the victim company, the defendant downloaded and stole proprietary computer source code for several medical software programs. The software programs stolen by the defendant were extremely sophisticated and very valuable. One set of software programs was designed to help radiologists locate and diagnose cancerous tumors on medical imaging scans. Another software program was used by hospitals to manage all of their large-scale data needs, such as medical information, admissions, and billing. Notably, some of the software programs stolen by the defendant were so sensitive that they had not yet even been released commercially.

The defendant continued his illegal downloading and stealing all the way up until his last days of employment with the victim company, and only one week before he was scheduled to return to his native China. He was caught only after an alert co-worker saw the

defendant downloading massive amounts of data onto his personal hard drive. A subsequent search of the hard drive confirmed the scope of the defendant's theft of trade secrets. For the defendant's illegal conduct in this case, the defendant deserves a term of imprisonment. The government respectfully requests that the Court sentence the defendant within the advisory guidelines range of 37 to 46 months.

Background

A. Facts

The defendant is a citizen of the People's Republic of China, and at the times relevant to the information, he was in the United States legally on a work visa. At the time of the offense, the defendant was employed at an international corporation that, among other things, developed: (1) medical imaging software that is used to aid medical professionals in spotting and diagnosing tumors; and (2) hospital administration software used to manage the massive amounts of data necessary to running a hospital. The defendant worked at offices located in Chester County, Pennsylvania, which is located in the Eastern District of Pennsylvania.

During the time period relevant to the information, the defendant worked in the business units responsible for developing the above-mentioned software, and was responsible for working as a computer technician supporting the units' computer networks. Although in the defendant's capacity as a computer network technician, he was given access to the source code for the medical software, he was not employed as a computer programmer for the company, and he had no legitimate business reason to access source code or to copy it. In other words, his job was to support the computer networks used by the computer programmers and other personnel responsible for developing the software products.

The computer source code copied by the defendant consisted mostly of Computer Assisted Design ("CAD") medical software, used by radiologists to help locate tumors and other medical problems. Specifically, this software is capable of "reading" radiology scans to help the radiologist identify body parts, and note areas of potential concern for the radiologist. The defendant also copied computer source code for software used by hospitals to manage the administration of the hospital, including managing medical data, billing, admissions, etc. The defendant also downloaded computer source code used by hospitals to generate passwords to access this information in the software. While some of the software was already being sold, some of the medical software products being developed by these business groups had not yet been released at the time of the defendant's unlawful copying. At the time of events in the information, all of this software was either already being sold in markets around the world, or was being developed for sale in those markets.

Over the course of many months, between in or about September 2008 through on or about February 28, 2009, the defendant accessed the internal corporate network containing the computer software source code using a password issued to him by the company. He then copied the computer source code for the medical software, without authorization from company, onto his own personal portable hard drive. The computer system that houses the source code is under very tight security. Access is limited only to specific company personnel through the use of a registered password. Additionally, each system available to employees has an access list which further restricts a persons access to particular areas. The defendant's access was based on the business units to which he was assigned. The computer systems which the defendant accessed are not accessible or available to individuals outside of the company.

In the last copying session, the defendant copied the software only a few days before he was scheduled to stop working at the company and return to China. To locate the source code he wanted to copy, the defendant asked a co-worker in which directories certain source code was stored. During this last downloading session from the company network to his personal hard drive, which took place at the company's offices, he downloaded the software covertly, hiding the downloading process on his computer monitor to prevent his co-workers from seeing what he was doing. He was unsuccessful, however, because one of his co-workers noticed that huge amounts of data were being copied by the defendant onto his personal hard drive. The defendant's actions were also suspicious because, at that time, the defendant had no official business duties, but should have been preparing to return to China. The defendant expected to take the portable hard drive, including all of the copied files, back with him to China.

After it was confirmed that the defendant was in fact surreptitiously downloading source code and other documents, the defendant was confronted by company personnel. The defendant fully admitted that he had taken the source code without authorization, and apologized for his actions. He left the business and later received a call from the FBI asking if he would agree to speak with them. He subsequently spoke to FBI agents voluntarily, wherein he again admitted that he downloaded company source code, and acknowledged that the company neither authorized him to copy it, nor would it have granted such authorization had he asked for it. A search warrant executed by the FBI on the defendant's portable hard drive confirmed the specific computer source code copied by the defendant.

Although the defendant was not employed at the company as a computer programmer, he did have training and education as a computer programmer. He thus understood

that copying source code for a software program could allow another company to create a similar software product without having to expend the same time or resources required by the owner of the source code.

B. Procedural History

On February 27, 2009, a complaint and warrant was issued for the defendant, charging him with offenses related to his theft of trade secrets from the victim company. On June 24, 2009, the defendant was charged via information with one count of theft of trade secrets and attempted theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(2) & (4). On July 23, 2009, the defendant waived prosecution by indictment and plead guilty to the single count in the information. The defendant plead guilty pursuant to a written plea agreement.

Sentencing Calculation

A. Statutory Maximum Sentence

The defendant could be sentenced to the following statutory maximum sentence: ten years imprisonment, 3 years of supervised release, a fine of $250,000 and a special assessment of $100.

B. Sentencing Guidelines Calculation

1. PSR Calculation

According to the Presentence Report of Investigation (PSR), the advisory guideline range is 57 to 71 months imprisonment, calculated as follows: (1) pursuant to U.S.S.G. § 2B1.1, the base offense level for the offenses is 6; (2) pursuant to U.S.S.G. § 2B1.1, the offense level is increased by 18 levels because the total loss amount was between $2.5 million and $7 million; (3) pursuant to U.S.S.G. § 2B1.1(b)(5), the offense level is increased by 2 levels because

the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality or foreign agent; (4) pursuant to U.S.S.G. § 3B1.3, the offense level is increased by 2 levels because the defendant abused a position of trust, (5) pursuant to U.S.S.G. § 3E1.1, the offense level is decreased by three levels because the defendant accepted responsibility for his crimes in a timely fashion. The total offense level is therefore 25. The defendant is in Criminal History Category I.

2. Objections to the PSR

The government has the following objections:

1. Paragraph 25: The PSR includes a two-level enhancement under U.S.S.G. § 2B1.1(b)(5) because the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality or foreign agent. The basis for this enhancement is the fact that the defendant attempted to steal the trade secrets of the victim company only a few days before he was scheduled to return to China. With respect, the government does not believe that this enhancement is appropriate because there is no evidence in the record to support it. For example, there is no evidence that the defendant was working with any foreign entities when stealing the trade secrets, or that he intended that the trade secrets would be provided to any foreign entities once he returned home to China. The PSR's conclusion is based on speculation rather than evidence. Absent any such factual support, the government does not believe that this enhancement is appropriate.

2. Paragraph 26: The PSR includes a two-level enhancement for abuse of a position of trust because the defendant utilized his corporate password to obtain access to the

trade secrets, and therefore violated the trust the victim company placed in the defendant. Again, with respect, the government does not believe that this enhancement is appropriate.

In deciding whether a defendant holds a position of trust, a court must consider: "(1) whether the position allows the defendant to commit a difficult-to-detect wrong; (2) the degree of authority which the position vests in [the] defendant vis-á-vis the object of the wrongful act; and (3) whether there has been reliance on the integrity of the person occupying the position." United States v. Pardo, 25 F.3d 1187, 1192 (3d Cir.1994); United States v. Dullum, 560 F.3d 133, 140 (3d Cir. 2009); United States v. Lieberman, 971 F.2d 989, 993 (3d Cir. 1992) ("[T]he primary trait that distinguishes a person in a position of trust from one who is not is the extent to which the position provides the freedom to commit a difficult-to-detect wrong." (internal quotation marks omitted)). "These factors should be considered in light of the guiding rationale of the section-to punish 'insiders' who abuse their positions rather than those who take advantage of an available opportunity." Pardo, 25 F.3d at 1192.

Under the specific facts of this case, the government does not believe that the defendant's position was one that qualified as a position of trust. While it is certainly true that the defendant had access to the trade secrets, he was not vested with the type of authority that would allow him easily to carry out and hide his involvement in the crime. The defendant was a computer technician assigned to manage the computer network, but could not exercise any control over the trade secrets. He was not, for example, a computer programmer or a supervisor with managerial control over the trade secrets. Indeed, it was the defendant's inability to carry out the crime in secret that ultimately led to his arrest. The government does not believe that the

mere fact that the defendant had legitimate access to the trade secrets because of his corporate password is sufficient to support this enhancement.

* * *

Without these two enhancements, the defendant would have a total adjusted offense level of 21 and a criminal history category I, resulting in an advisory guidelines range of 37-46 months. The government respectfully requests that the Court find this to be the applicable advisory guidelines range, and to sentence the defendant to a term of imprisonment within that range.

Analysis of Sentencing Factors

A thorough consideration of all of the sentencing factors set forth in 18 U.S.C. § 3553(a) indicates that the most appropriate sentence is one within the advisory guidelines range of 37 to 46 months.

The Supreme Court has declared: "As a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark." Gall v. United States, 128 S. Ct. 586 (2007). Thus, the Sentencing Guidelines remain an indispensable resource for assuring appropriate and uniform punishment for federal criminal offenses.

This Court must also consider all of the sentencing factors set forth in Section 3553(a). Those factors include: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (3) the need to afford adequate deterrence to criminal conduct, and to protect the public

from further crimes of the defendant; (4) the need to provide the defendant with educational or vocational training, medical care, or other correctional treatment in the most effective manner; (5) the guidelines and policy statements issued by the Sentencing Commission; (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and (7) the need to provide restitution to any victims of the offense. 18 U.S.C. § 3553(a).

A. Consideration of the 3553(a) Factors

1. The nature and circumstances of the offense and the history and characteristics of the defendant

The nature and circumstances of this offense are serious. The defendant downloaded and stole extremely valuable computer source code for several medical software programs. The defendant did so with the full knowledge of what he was stealing, and the great damage he could have caused to the victim company had these trade secrets been disclosed to the marketplace. The Court should impose a sentence that recognizes the severity of the defendant's crimes. With respect to the history and characteristics of the defendant, this appears to be his first criminal offense, although little is know about the defendant because he a Chinese citizen here in the United States on a short-term work visa. Overall, the government respectfully requests that the Court impose a sentence within the advisory guidelines range of 37-46 months.

2. The need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense.

A within-guidelines sentence would reflect the seriousness of the offense, promote respect for the law, and adequately punish the defendant for his criminal behavior. As

described above, the defendant engaged in a serious offense. Trade secrets must be protected to preserve the healthy competitiveness of business and industry and promote free enterprise in the marketplace. Allowing defendants who are guilty of such crimes to escape serious punishment would threaten those ideals. A sentence within the advisory guidelines range would properly reflect these considerations and communicates to the defendant and society that the justice system will not tolerate this type of criminal behavior.

3. The need to afford adequate deterrence to criminal conduct, and to protect the public from further crimes of the defendant.

A sentence as requested by the government is necessary to deter other potential trade secret thieves and protect the public from further criminal activity of the defendant. This type of crime is all too easy to commit; anyone with access to trade secrets within a business conceivably could steal that trade secret. Those who are inclined to engage in it must be deterred by the possibility of receiving a serious sentence. The defendant himself also must be deterred from engaging in this type of illegal activity. The recommended sentence will achieve this objective.

4. The need to provide the defendant with educational or vocational training, medical care, or other correctional treatment in the most effective manner.

There is no need in this case to adjust the sentence in order "to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner . . . ." Id. § 3553(a)(2)(D).

5. The guidelines and policy statements issued by the Sentencing Commission and the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct.

While the sentencing guidelines are advisory, they remain the sole means available for assuring some measure of uniformity in sentencing, fulfilling a key Congressional goal in adopting the Sentencing Reform Act of 1984. Reference to the guidelines, while carefully considering the 3553(a) factors particularly relevant to an individual defendant, is the only available means of preventing the disfavored result of basing sentences on the luck of the draw in judicial assignments. The Third Circuit explained:

> Even under the current advisory system, district courts must "meaningfully consider" § 3553(a)(4), i.e., "the applicable category of offense . . . as set forth in the guidelines." The section of *Booker* that makes the Guidelines advisory explains that "the remaining system, while not the system Congress enacted, nonetheless continue[s] to move sentencing in Congress' preferred direction, helping to avoid excessive sentencing disparities while maintaining flexibility sufficient to individualize sentences where necessary." Booker, 543 U.S. at 264-65 (emphasis added). The Guidelines remain at the center of this effort to "avoid excessive sentencing disparities," and, as the Booker Court explained, the Sentencing Commission will continue "to promote uniformity in the sentencing process" through the Guidelines. Id. at 263. We have likewise observed that the "'Guidelines remain an essential tool in creating a fair and uniform sentencing regime across the country.'" Cooper, 437 F.3d at 331 (quoting United States v. Mykytiuk, 415 F.3d 606, 608 (7th Cir. 2005)).

United States v. Ricks, 494 F.3d 394, 400 (3d Cir. 2007) (emphasis in original). Therefore, the Supreme Court has held that "district courts must begin their analysis with the Guidelines and remain cognizant of them throughout the sentencing process" in order to assure fair, proportionate, and uniform sentencing of criminal offenders. Gall, 2007 WL 4292116, at *7 n.6.

In accordance with the purpose of the guidelines, it is part of our sense of justice that similarly situated defendants should be given similar sentences. This defendant should just

as lengthy a term of imprisonment just as if he had stolen more than $2.5 million in cash. The sentencing guidelines provide a recommended sentencing range which similarly situated defendants receive as punishment. This Court should consider those guidelines when determining the appropriate sentence for the defendant.

Conclusion

The defendant carried out a serious crime. For all the reasons set forth above, this Court should impose a sentence that is within the advisory guidelines range of 37 to 46 months.

Respectfully submitted,

MICHAEL L. LEVY
UNITED STATES ATTORNEY

/ Leo R. Tsao
LEO R. TSAO
Assistant United States Attorney

CERTIFICATE OF SERVICE

I certify that on this date a copy of the Government's Sentencing Memorandum filed under seal was served by electronic filing and first class mail on the following defense counsel:

Catherine Henry, Esquire
Defender Association of Philadelphia
Federal Court Division
The Curtis Center Building
601 Walnut Street
Suite 540 West
Independence Square West
Philadelphia, PA 19106

/ Leo R. Tsao
LEO R. TSAO
Assistant United States Attorney

Date: October 30, 2009